Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 6.017

IJCSMC, Vol. 6, Issue. 5, May 2017, pg.373 – 387

An Assessment of the Level of Information Security Awareness among Online Banking Users in Nigeria

[1]Dr. Amit Mishra, [2]Ayesha. Awal, [3]Joseph Elijah, [4]I. Rabiu

[1,5]Deptt. of Mathematics/Computer Science Ibrahim Badamasi Babangida, University, Nigeria

[1] i.amitmishra@gmail.com, [2] meeayeesha@yahoo.com, [3] elijoe3yk@gmail.com, [4] idrisrabiu76@yahoo.com

Abstract:
Internet is an important and valuable tool for many successful businesses in this 21st century thereby keeping a huge amount of information at ones' fingertips, the introduction of Internet banking system has classically replaced most of our previous banking system. Internet banking also called online banking has helped in production growth, quick access to ones' account, smooth and easy transactions of goods and services. Since the introduction of online banking to Nigeria, the banking sector has experienced huge development in their mode of operations and services. However, online banking system is facing some problems in financial information security. Financial information security threats are these problems which mostly affects online banking users who input their confidential financial details online. Therefore, to prevent them from been a victim of security threat (information breach), there must be proper awareness about financial information security which will help in protecting online banking users from any form of attack. In order to provide sound awareness about financial information security, a survey is carried out using questionnaires and interview to assess online banking users about their level of awareness in financial information security. From the analysis of the survey it was observed that most online banking users in Nigeria are still not aware of various attacks associated with online banking, which means the existing method of awareness are feeble.

Background

Internet banking (Online banking) is a system where by goods and services are transact on the cyber space, these transactions includes paying bills, paying mortgages, checking account balance, transferring funds, and purchasing all kind of goods. With this technological advancement bank customers need not to go bank before they make their transactions. Internet banking users can access their accounts from a browser and software that runs internet banking programs anywhere on the bank's world wide web server, using their devices like desktop computer or mobile devices (such as smart phone, palm top, laptop and so on). Which means, bank customers' confidential information moves from their device through network to their Banks' server when performing online banking.

However, customers' confidential information is always the target of attackers. These attackers use to develop different methods of attacks to hack into online banking user's financial information so that they can have control over the account.

Phishing is one of the methods attackers uses to get confidential bank information from online banking users, phishing is a method of internet fraud that is use to hijack confidential information (such as credit cards, user identity, pin number and password) from internet users. Phishing is done by creating a fake web site replica to the legitimate bank of the target customers asking them through e-mail or text message to log in into the web site to input their confidential bank information, after the customer have submit their confidential information, they will now redirect the customers to their legitimate bank website to avoid detection.

It is mandatory for every bank to create information security awareness for their customers so that they will not fall victim of any kind of information breach. With constant awareness, online banking customers will be protected against any latest threat, which means sound information security awareness will keep online banking users protected at all time, by educating them on different kind of threats, how to detect a threat and how to tackle them when encountered. This research aims at assessing the level of information security awareness among online banking users in Nigeria, and also give answers to different questions pertaining to information security awareness.

Problem Statement

The problem of online banking threat is growing day by day, whereby cyber criminals design different methods to gather valuable resources online, such as customer details and confidential bank information, so that online businesses will ruin-down. Many organizations, sole-proprietorship and individuals have fell victim of this threats where some of them crashed and some experience low income as a result of dwindle capital or resources. The main thing these cyber criminals are interested in is to steal internet banking users' identity, using a particular method suitable for them, so as to gain sensitive information from online banking users during their online transactions, which will be used later to attack those individuals and organizations.

During online transactions, confidential matters move from senders to the receivers, eavesdroppers might be somewhere listening to their communications, whereby breaches of privacy and access to confidential information may occur without users' consent, some users may

not be aware of the vulnerability due to inexperience or the threat is new to them so they might not know how to prevent it. Therefore, the need for up-to-date security measures is an important system that should be put into cognizant for self-protection by government, businesses and individuals.

This study defines information security awareness for online banking users as informal training and knowledge given to internet banking users so as to expose them to sound information security measure on how to tackle any security threats associated with online transactions.

LITERATURE REVIEW

Introduction

This literature review aims to explain the terminologies associated with online transactions and online banking threats, such as Malware attack, Phishing attack, Key logger, and so on. It will also elaborate the literature of the above-mentioned threats, different ways in which online banking users can be attacked through their devices such as desktops, laptops and telephones and provide possible solution to them.

Online Transactions and Online Banking Threats

This section will discuss the definitions of online banking transactions and online banking threats with their possible way out.

Online transactions

This is the act of conducting or carrying out business, negotiations, plans and exchange of goods and services on the cyber space (Internet), some terms are associated with online transactions which are; e-payment, e-banking, e-business, e-commerce, and online banking. Below is the definition of each terms:

Electronic payment (e-payment) is the process of exchanging monetary value between two or more people in business transactions and transmitting this value over the internet using a supported device. This system allows financial information to be held, processed, received, and transferred in a digital form.

Electronic banking (e-banking) is an act of delivering goods and services directly to the customers through an electronic device, which means transactions can be done anywhere provided you have an electronic device that runs the internet banking system, this is different from the traditional banking system which you have to go to the banking hall before you make your transactions. E-banking can be done on these devices or platforms which are; telephone banking, mobile phone applications, BPAY and BPAY view, NetBank (Internet Banking), ATM, Debit MasterCard, key card (debit card), MasterCard and Visa Plus networks, and AFT (Automated Funds Transfer).

Electronic business (e-business) E-business are processes which includes sending e-mails to staff or suppliers, performing online transactions, using internet for selling goods to consumers, monitoring and exchanging information, auctioning surplus inventory and collaborative product design.

Electronic commerce (e-commerce); is the act of transaction between firms and individuals which involve exchange of money, good or duties such as shipping, billing and payment information. The concept of doing this electronically or online bring about E-commerce.

Online-banking or Internet-banking is a new age banking system using internet technology as it delivery channel to conduct banking activities. This system allows customers to manage their financial accounts and transactions, such as money transfers, bill payments, personal information updating, and balance checking through the Internet, anywhere the access is available and any time. Internet banking service is now becoming more accepted since it provides convenient and efficient service to the bank customers, it also helpful to the bank due to the large numbers of their customers by reducing the crowd that may accumulate in the bank.

Online banking threats

These are attacks carried out on the cyber space threatening the online banking users, unlike the traditional banking system which attacks can only be done physically in most cases. Online banking threat is also referred as cyber-attack and the attackers are called cyber-criminals or hackers. Cyber criminals are developing more sophisticated tools to hijack customers' financial information sometime through the banks or the customers themselves. The following threats are associated with online transactions, the difference between them and their preventive measures are explained below:

Malware Attack

Malware attack is a malicious software that is designed to cause damage on stand alone or networked computers. The cyber-criminals use different types of malware base on the operation at hand. There are malwares that can cause damage to device being used for online banking (such as desktop, laptop, PDA, palm top and smartphone) and there are some malwares that are meant for stealing confidential information of internet users. Malware threats in online banking can come in form of Trojan, which causes damage by obstructing or slowing down the security structure of a personal device. Malware can be prevented by having antivirus software installed on personal devices which is used to run internet banking to avoid untrusted link from downloading, scanning a personal device before engaging in an online transaction and avoid using someone's personal device for online transactions.

Key logger

Key logger also referred as keystroke logger or system monitor is a hardware or software that monitors each keystroke a user types on a specific computer's keyboard. If hardware made of key

logger is plug into the victim computer by hacker, all information that the victim typed during online transaction will be available on the key logger.

Identity theft

Identity theft is a method of attack in which attacker hijack someone's identity in order to gain access to the person's resources and other valuable things using the person's identity. This attack is successful when the attacker have little information about the victim, and will use this information to perform illegal transaction on the victim's account acting like the legal owner of the account. This attack normally occurs when attacker has gotten information like password, PIN number and so on. Identity theft can be avoided by strongly guiding financial information such as password and PIN.

Phishing

This is an act whereby internet banking users are sent bogus emails that lure users to Internet sites that resemble their legitimate bank sites attempting to obtain user's information such as account number, PIN number, Password, account name and so on. The best way to protect one's self from phishing is to recognize a phish.

Man-in-the-Middle Attack (MitM)

Man in the middle attack is a type of attack whereby the hacker impersonate each endpoint to the satisfaction of the other by active interception of confidential information hackers makes an independent connection between two victims, making them believe they are communicating with each other over a private network while the hacker is receiving the messages between them and controlling the whole conversation, modifying the message and retransmit without the knowledge of the sender or receiver.

Man-in-the-Browser (MitB) is a Trojan horse program, which infects the user's internet browser and inserts itself between the user and the Web browser, modifying and intercepting data sent by the user before it reaches the browser's security mechanism. It operates without any detectable signs to the user or the host application using a Trojan program to intercept and modify the transactions, and then redirect it into the attacker's account, this attack can be avoided using a secure Web browser from the bank or by installing any trusted anti-virus that have strong malware detection which will monitor both the device and web browser.

Shoulder surfing

Shoulder surfing is the direct observation method which involve looking over one's shoulder to get vital information like obtaining password and Pins. Shoulder surfing can be avoided by guarding one's private information consciously when inputting them online, that is looking around before typing in financial information and carefully watch one's surrounding.

RESEARCH METHODOLOGY

The purpose of this study is to assess online banking users' level of awareness about threat associated with online banking and their knowledge about financial information security. The

selected methodology in this study was approached by descriptive research and comparative research. Descriptive research can require either or both quantitative or qualitative method to find out what might be applied to investigate the collecting questions.

Research Methods

This Quantitative and qualitative research method are commonly described as the basic frameworks for academic social researchers, although the distinctions between the two must be understood. The goal of quantitative research is to measure and analyze causal relationships between variables within a value-free framework. Qualitative research approach also make it easier to understand any scenario that needs to be viewed within its context. For instance, statistical data collected from a quantitative approach will shape the interview questions for the qualitative aspect of the study.

Quantitative Research

Quantitative research deals with the numerical form of data obtained from the respondents, quantitative approach using survey method aim to measure demographic and personal attributes, living conditions and circumstances, behavior, opinions, attitudes, and values.

Mixed Methods Research

The introduction of mixed method has assist the researcher to consider research questions from different perspectives, mixed methods have been widely used for research projects. The purpose of mixed method in this research is to combine quantitative and qualitative data together for good analysis so as to achieve answers to the research questions.

Research design (Plan)

The technique in selecting the right investigative methods is very important when developing a research design (Plan) since it assist in developing an appropriate design. An appropriate research design is essential as it determines type of data, data collection techniques, tools and sample group. Research design is the function of research objectives, it can also be defined as set of advance decisions that makes up the master plan, specifying the methods and procedures for collecting and analyzing the information needed. This study was conducted in eight phases. Phase one was the feasibility study, which includes gathering information from the existing security system and literature review. Phase two deals with design techniques and tools to be used in the study. Phase three evaluated the reliability and validity of the phase two. Phase four executed a pilot test of the previous phases. Phase five completed the actual survey (Data gathering). Data was collected from various sources, from interviews and questionnaires administered to respondents. Phase six involved description and statistical data analysis, with cross-tabulations of gathered data in phase five. Phase seven and eight deals with documentation of reports based on findings and provide possible solutions that will solve the problems.

Feasibility Study

This research began with exploring the previous research to collect some existing information, which provide the study an essential background information needed to proceed with the research. The exploratory study reviewed previous research, explored new and related information which was incorporated into this research. This research established the scope of the study by forming questions. The questions were about the problems or the situation of state or conditions and their relationships with the respondents' knowledge and behaviour in online banking and threats.

Research Approach/Technique

This involved selecting appropriate techniques and tools to be used in the research. Sample group was also part of this phase. The next paragraphs describe the data collecting techniques, tools, and details of selecting a sample group.

Data Collection Techniques and Tools

Data collection techniques allows the study to collect information systematically, the objects of the study are (people, objects, scenario) and about the settings in which they happen.

Table 1. Data Collection Techniques and Tools

Data Collection Techniques	Data Collection Tools
Administering questionnaires	Questionnaire
Interviews (Groups and Individuals)	Questionnaire, structured interviews, and open-ended interview

Evaluation of Reliability and Validity of Tools & Techniques

This phase, the academic supervisor of this study was consulted for review of the tools and techniques that will be used and he confirm the validity of this phase. After the review process, the tools and technique were ready for pre-test in an exploratory survey.

Actual Survey (Data Gathering)

This phase deals with data collection using the concept of group interviews and individual interviews with distribution of questionnaires to respondents across the four-selected state in Nigeria, which was the medium for the data collection and gathering.

DATA ANALYSIS AND RESULTS

This section represents the analysis of the data, both quantitative and qualitative which was extract from the questionnaires, open-ended questions and interviews so as to provide answers to the research questions. This section consists of six descriptive results of the survey and new methods of improving information security awareness, this includes;

Background of the respondents.

Out of the 200 questionnaires distributed, 196 were fill correctly, 2 invalid and 2 was not retrieved. The correctly filled were fully evaluated and analyzed, the following paragraphs will discuss the background of the respondents in detail.

Respondents Gender

All respondents are resident of Nigeria, the distribution of the questionnaires are summarized in the table below.

Table 2 showing gender distribution of the survey to respondents.

Gender	Frequency	Percentage
Male	101	50.5%
Female	95	47.5%
Valid Total	196	98%
Invalid	2	1%
Not Retrieved	2	1%
Overall Total	200	100%

The data above shows that the percentage of males and females in the sample were 50.5% and 47.5% respectively. The population surveyed has a gender distribution closely equal which means both party (Male and Female) use online banking.

Respondents' Age

Table 2 showing age distribution of the survey to respondents.

Age	Frequency	Percentage
Below 20	18	9%
20 – 25	24	12%
26 – 35	52	26%
36 – 44	46	23%
45 – 50	34	17%
Above 50	22	11%
Invalid / Not retrieved	2 / 2	2%
Total	200	100%

From table 2, above it shows that most of the respondents were within the age bracket of 26-35 at 26% followed by the group aged between 36-44 at 23%, and the 45-50 years at 17%. The next age group was 20-25 years at 12%, above 50 at 11% and below 20 at 9%. From the analysis of the table above it shows that respondent within the age bracket of 26-35 use online banking most.

Occupation Classification of Respondents

Table 3 below shows the classification of respondents' occupation which was gathered from the questionnaires administered to them.

Occupation	Frequency	Percentage
Instructors	20	10%
Students	34	17%
Managers	14	7%
Technicians	32	16%
Workers	46	23%
Laborers	15	7.5%

Home duties	14	7%
Retired	21	10.5%
Invalid / Not retrieved	2 / 2	2%
Total	200	100%

Table 3 above shows the occupations of the respondents. All the occupations are paid excluding student, retired, and home duties, which are unpaid occupations, but were given some incentive Instructor is a category of professional job such as academic lecturers, IT specialists, consultants, building engineers and so on.

Education Level of the Respondents (Education Status)

Table 4 below shows the highest education status of the respondents

Education Status	Frequency	Percentage
PhD / Dr.	10	5%
Master degree	18	9%
Bachelor degree	54	27%
Diploma	46	23%
N C E	56	28%
Secondary School Graduate	12	6%
Invalid / Not retrieved	2 / 2	2%
Total	200	100%

Table 4 above shows that the highest current education level of the respondents in this sample were National Certificate of Education with (28%) followed by Bachelor degree with (27%) and Diploma at (23%).

This section described the background of the respondents in terms of genders, ages, occupations and education levels. The results have been analyzed and from the findings it reveals that male respondents used online banking more than females. The majority of the respondents in this survey were in the age bracket of 26-35 and most respondents are workers. In addition, most respondents' education level (Status) is National Certificate of Education (NCE).

Experience of the respondents in using online banking.

In this section, the respondents' behaviors in accessing online banking services will be discussed.

General experience about online banking services

Out of the 200 questionnaires administered during the survey, 196 responses were collected, 146 respondents at 74.5% had experience in accessing online banking services, while 50 respondents at 25.5% had never experienced online banking before due to some reasons. This reasons are provided in figure 4.3.3, and their comments were discussed in the following paragraph.

Table 5 below shows online banking users and non-online banking users.

	Frequency	**Percentage**
Online banking users	146	74.5%
Non-online banking users	50	25.5
Total	196	98%

Reasons for using online banking

Those that are using online banking services were given the opportunity in the questionnaire to select multiple reasons for using online banking. From their responses 46 online banking respondents at 31.5% indicated that they used online banking services because of the swift and accuracy of their transactions. 40 respondents with 27.5% said due it convenient in terms of 24/7 access anywhere provided there is internet connection, 32 respondents at 21.9% revealed that it saves time in terms of not going to the bank before you make transactions and save them from waiting on a queue in the bank, amazingly, only 12 respondents at 8.2% believed that online banking offered better security and 16 respondents with 10.9% felt that online banking also minimised some expenses which means it saves money. The percentage of respondents that chose swift and accuracy, convenience, and time saving are much compare to other reasons, which means these three factors are the major reasons why most online banking users welcome it. The table below shows respondents reasons for using online banking.

Table 6 showing respondents reasons for using online banking.

Reasons for using online banking		
Responses	**Frequency**	**Percentage**
Swift and Accuracy	46	31.5%
Convenience	40	27.5%
Time saving	32	21.9%
Higher responses Total	**118**	**80.9%**
Better security	12	8.2%
Minimise expenses	16	10.9%
Total responses	**146**	**100%**

Reasons for not using online banking

The reasons why some of the respondents have not been using online banking services, in sum total we have 50 respondents. From their responses. 23 respondents at 46% of the non-online banking respondents were concerned about the security of their financial information, whereas 10 respondents at 20% indicated that they were not aware of online banking. Also, 11 respondents at 22% revealed that they did not see any real value in using online banking or having an online banking account, 4 respondents at 8% said they are too young to have bank account (Under-age), where 2 respondents at 4% mentioned that they have not taken time to open an online banking account. Table 6 below shows reasons why some respondents had not used online banking services.

Table 6 Showing respondents reasons for not using online banking.

Reasons for not using online banking		
Responses	**Frequency**	**Percentage**
Concerned about the security	23	46%
Not aware of online banking	10	20%
Didn't see any real value of it	11	22%
Under-age	4	8%
Have no time to open an online banking account	2	4%
Responses Total	**50**	**100%**

Main activities carried out by the respondents when using online banking services. From their responses 74 respondents at 50.6% perform money transfer, where 56 respondents at 38.5% check their account balance and information, also 10 respondents at 6.8% update their personal information and 6 respondents at 4.1% perform other operations. Table 4.3.4 below lists these activities and shows the respondents according to the activity they perform most.

Table 7 Showing most activities carried out by the respondents when performing online banking.

Responses	**Frequency**	**Percentage**
Money transfer	74	50.6%
Checking balance and account information	56	38.5%
Update personal information	10	6.8%
Other	6	4.1%
Total responses	**146**	**100%**

This shows obviously, that most of the respondents didn't bother about regular updates of their personal information. However, it can be viewed that the main reasons why respondents used online banking were to transfer money, check their account balances, and make payment of their bills.

This section provides a clear description of respondents' experiences in using online banking services, it also explain their reasons why they use online banking and why they are not using it. It further describes the most activities the respondents use to carry out while using their online banking account.

From the overall result, it shows that the number of online banking respondents was greater than the non-online banking respondents.

The experience of the respondents' in respect of online banking security.

This section analyzes respondents' experiences with regard to online banking security. How the respondents protect their self against any form of attacks and the protections provided by their banks are discussed in this section.

Respondents' security protections installed on their devices

This part in the questionnaire deals with the respondents' security protection that was installed on their devices while performing online banking. It is likely some online banking users installed more than one type of security protection, which sometime they contradict each other. Table 8 below shows their responses.

Table 8 Showing different protections installed on respondents' devices

Responses	Frequency	Percentage
I installed firewall application	19	13%
I installed anti-virus application	48	32.8%
I have anti-spyware in my operating system	42	28.7%
I installed security protection but I don't kwon if it is working	11	7.5%
I am not sure if I have any security protection on my device	12	8.5%
I don't use any security protection	10	6.8%
Other	4	2.7%
Total responses	**146**	**100%**

Security protections provided by the respondents' banks when accessing online banking

This section discusses the types of protections provided by respondents' banks when accessing their online banking accounts using different authentications. Majority of the respondents were required to use a login password authentication, with frequency of 82 at 56.2%. Also, some respondents' banks use login password with mobile (SMS) verification code, which was the second highest with frequency of 44 at 30.1% and other respondents were required login password with security questions, with the frequency of 16 at 11%. Furthermore, some respondents with frequency of 4 at 2.7% access their online banking account using biometric security which this service is done mostly in respondents' bank branch since it seems to be the newest type of authentication security. Table 9 below shows the security protections provided by the respondents' banks when accessing online banking.

Table 9 showing the security protections (Online authentications) provided by the respondents' banks when accessing online banking.

Responses	Frequency	Percentage
Login password	82	56.2%
Login password with mobile (SMS) verification code	44	30.1%
Login password with security questions	16	11%
Biometric security	4	2.7%
Total responses	**146**	**100%**

Perception and experience of the respondents towards online banking attacks.

This section analyzes the respondents' experiences and their knowledge about online banking threats and how to decrease the risks. However, with the responses gathered from the questionnaires, this research was able to analyze the responses based on findings. The findings are explained below in tables and charts with their frequency values and percentages.

Respondents awareness about risk or threats associated with online banking

Majority of the online banking users were not fully aware of online banking threats, 106 respondents at 72.6% out of the 146 respondents that use online banking were partially aware of the online banking threats while 32 respondents at 21.9% are fully aware of the threats and 8 respondents at 5.5 were not aware, the percentages of the partially aware and not aware is bigger than those that are fully aware, therefore this shows that the previous method of awareness is weak. The following paragraphs present in tables and charts the respondents' awareness about online banking threats and the medium in which they got the awareness.

Table 10. Showing respondents awareness about risk or threats associated with online banking

Responses	Frequency	Percentage
Yes am fully aware	32	21.9%
Yes am partially aware	106	72.6%
I am not aware	8	5.5%
Total responses	**146**	**100%**

Respondents medium of awareness

From the responses gathered from the questionnaires, most of the respondents get their awareness through mobile (SMS), this equated 36.5%, followed by Email alert which also equated 21.9%, other mediums are presented in the table below with their frequencies and percentages.

Table 11 Showing respondents medium of awareness.

Responses	Frequency	Percentage
Newspaper	8	5%
Television	6	4.5%
Mobile (SMS)	53	36.5%
Internet	11	7.5%
Email	32	21.9%
Bank	20	13.6%
Friends	10	6.8%
Other	4	2.7%
Total valid responses	**144**	**98.5%**
Not specify	2	1.5%
Total responses	**146**	**100%**

Respondents experience about some selected online banking threats.

The table 12 below presents respondents experience about some selected online banking attack, using percentage to know their level of experience.

Table 12 showing respondents experience about online banking attacks.

Threats	Respondents frequencies and their level of awareness in percentage											
	F	0%	F	10%	F	20%	F	50%	F	70%	F	100%
Phishing	10		15		35		55		20		11	

Malware Attack	77	34	15	9	6	5
Shoulder surfing	0	1	3	11	29	102
Man-in-the-Middle Attack	92	33	11	5	3	2
Identity theft	4	11	20	45	22	34

Note; in the table, F denote frequency of the respondents.

From the table above it is seen that most of the respondents are fully aware of only shoulder surfing since it is the common attack done by the cyber criminals, other attacks which are sensitive need to be given a lot of consideration by providing more reliable ways to educate online banking users against these attacks.

Respondents experience about online banking attacks

The responses gathered from the questionnaire shows that 12 out of the 146 online banking users had been attacked on their online banking account before. The table below presents different experience of the respondents and their actions towards it.

Table 13 showing respondents scenario of attack.

Scenario	Action taken	Frequency	Percentage
I noticed some transactions appearing on my credit card every month	I visited my bank to rectify the problem	1	8.3%
My account is been hacked into through downloading a software which happen to be a malware	I uninstalled the software and delete all it directories, then scan my device with anti-virus	1	8.3%
My credit card was collected forcefully by criminals and I was asked to provide my pin for unwanted withdrawal	I visited my bank to rectify the problem by destroying the credit card	3	25%
My account is been hacked into, through an email that requested my login details	I visited my bank to rectify the problem	7	58.5
Total responses		**12**	**100%**

CONCLUSION

This research has analysed the level of information security awareness of online banking users in Nigeria using questionnaires and interviews. The responses of the respondents helped the study to propose new methods of improving information security awareness. This research work focused on the way or method in which information security awareness can improved, and to reduce or eradicate the cases of financial information breach, using the new proposed methods of spreading information security.

REFERENCES

10 Tips to Prevent Phishing Attacks. http://support.pandasecurity.com/blog/security/10-tips-prevent-phishing-attacks

A. M. French, "A Case Study on E-Banking Security – When Security Becomes Too Sophisticated

attack during communication between a mobile devices and the back end user in mobile banking application," IOSR Journal of Computer Engineering, vol. 16, pp. 35-42, April 2014. Computer & Security, vol. 25, pp. 289-296, Feb. 2006.

Essays, UK. (November 2013). Effectiveness of information security awareness information

F. A. Aloul, "The Need for Effective Information Security Awareness." *International Journal of* for the User to Access Their Information," *Journal of Internet Banking and Commerce*, vol. 17, No.2, pp. 3-13, August 2012.

H. A. Kruger, W. D. Kearney, "Aprototype for assessing information security awareness," https://sqnetworks.com/downloads/AhnLab_AOS_WhitePaper.pdf *Intelligent Computing Research*, vol. 1, pp. 130-137, June 2010. W. Candid, "Threats to Online Banking," Symantec, Symantec security response, white paper, 2005.

L. Anthony, K. Stephen and K. Micheal, "Identify threats associated with Man-in-the-middle Online Security: Online Banking, the Threats and Countermeasures. Available: technology essay. http://www.ukessays.com/essays/information-technology/effectiveness-of-information-security-awareness-information-technology-essay.php?cref=1

What are the dangers of online banking? Available: http://blogs.norman.com/2013/for-consumption/what-are-the-dangers-of-online-banking

